Descripción del servicio

Estándar de seguridad de datos del sector de tarjetas de pago

Consultoría sobre correcciones

Contenido

Servicio de correcciones relacionadas con el PCI DSS

SecureTrust™ es una división de Trustwave Holdings, Inc.

DESCRIPCIÓN DEL SERVICIO

El servicio de consultoría sobre correcciones relacionadas con el Estándar de seguridad de datos del sector de tarjetas de pago (Payment Card Industry Data Security Standard, PCI DSS) (el "Servicio") se diseñó para ayudar y orientar a las organizaciones para lograr cumplir con el PCI DSS conforme a lo establecido por el Consejo de Estándares de Seguridad del PCI (el "Estándar") y mantener dicho cumplimiento.

Los términos en mayúscula que se utilizan en esta descripción del servicio, pero que no se definen en el presente documento, tienen el significado que se asignó en el Acuerdo maestro de servicios de Trustwave que se encuentra en https://www.trustwave.com/en-us/legal-documents/contract-documents/ o en un acuerdo similar celebrado entre SecureTrust y el Cliente.

CARACTERÍSTICAS BÁSICAS DEL SERVICIO

El Servicio incluye las siguientes características básicas:

Portal de SecureTrust

Una de las características del Portal de SecureTrust consta de, entre otras, la aplicación Compliance Manager para gestionar el proceso de cumplimiento, así como para recopilar y almacenar de forma segura las pruebas, la documentación y los productos finales.

Servicios globales de riesgo y cumplimiento

El equipo de Servicios Globales de Riesgo y Cumplimiento (Global Compliance and Risk Services, GCRS) está formado, entre otros, por los siguientes cargos y funciones clave:

Asesor de seguridad calificado (Qualified Security Assessor, QSA): es el principal recurso para el cumplimiento del Servicio y es responsable de realizar las actividades de consultoría.

Consultor de gestión (Managing Consultant, MC): brinda orientación, supervisa los proyectos e informa acerca de la gestión de calidad al QSA, además de actuar como punto de contacto secundario del Cliente en lo que respecta a derivaciones y consultas.

Comité de Revisión de Cumplimiento (Compliance Review Board, CRB): actúa como la autoridad final para la interpretación de los requisitos del Estándar o la resolución de inquietudes de cumplimiento complejas, al proporcionar uniformidad y continuidad en todas las evaluaciones de SecureTrust. El CRB también es la autoridad final de derivación para la resolución de problemas relacionados con el estado de cumplimiento de los requisitos del Estándar o la revisión de un control compensatorio.

Consultoría sobre correcciones relacionadas con el PCI DSS: consultoría y orientación para lograr cumplir con el Estándar y mantener dicho cumplimiento. SecureTrust le proporcionará al Cliente el Servicio

necesario para desarrollar planes y procesos de medidas prioritarias para la corrección de deficiencias de cumplimiento del PCI DSS.

PRESTACIÓN E IMPLEMENTACIÓN

Inicio del proyecto

El equipo de GCRS de SecureTrust facilita la prestación del Servicio, lo que incluye programar y llevar a cabo la reunión remota inicial para definir y acordar un plan de proyecto de alto nivel que cuente con fechas cruciales, pasos clave, estimaciones de duración, requisitos de recursos y procedimientos de derivación.

Consultoría sobre correcciones relacionadas con el PCI DSS

El QSA de SecureTrust y el Cliente colaborarán, y el QSA proporcionará orientación y recomendaciones para crear planes de acción prioritarios y abordar procesos de corrección de deficiencias de cumplimiento del PCI DSS. Algunas actividades del Servicio son las siguientes:

- La creación de un plan de medidas de corrección para controles ineficaces.
- El diseño de procesos y proyectos para corregir deficiencias conocidas para las áreas de mayor prioridad y de alto riesgo.
- El aprovechamiento de controles comunes en todo el entorno de control del Cliente para corregir las deficiencias identificadas.
- La determinación de las pruebas y la documentación necesarias para demostrar que se cumple con el PCI DSS.
- La identificación de los desafíos y riesgos clave del Cliente asociados con el cumplimiento del PCI DSS.
- El establecimiento de procedimientos de autoevaluación para que los propietarios de los controles los ejecuten en las áreas de alta prioridad.

SecureTrust llevará a cabo una reunión de cierre con el Cliente, si así lo desea.

RESPONSABILIDADES DE SECURETRUST

- Establecer contacto y permanecer a disposición para las comunicaciones con el Cliente.
- Establecer planes de comunicación y derivación.
- Crear una cuenta de Cliente en el Portal de SecureTrust.
- Definir un plan de proyecto de alto nivel que contenga fechas cruciales, pasos clave, estimaciones de duración y requisitos de recursos.
- Programar y llevar a cabo reuniones iniciales, periódicas de seguimiento y de cierre.

RESPONSABILIDADES Y CONFIRMACIONES DEL CLIENTE

- Establecer contacto y permanecer a disposición para las comunicaciones con SecureTrust.
- Establecer planes de comunicación y derivación.
- Acordar un plan de proyecto de alto nivel que contenga fechas cruciales, pasos clave, estimaciones de duración, productos finales y requisitos de recursos.
- Proporcionar de forma precisa toda la información necesaria, lo que incluye las partes interesadas clave, la información correspondiente del entorno del Cliente y los requisitos de configuración.
- Informar a SecureTrust acerca de todas las actividades de mantenimiento del entorno del Cliente y los cambios que podrían afectar el Servicio.

- Responder con precisión a las solicitudes de los equipos de SecureTrust al establecer contacto y recopilar información.
- Proporcionar detalles completos y precisos del entorno relevante y otros datos de las operaciones comerciales.
- Poner a disposición recursos capaces de participar en las actividades del Servicio.
- Participar en la explicación de los materiales durante las llamadas, las reuniones, las entrevistas, los debates, la inspección de instalaciones y los análisis de controles, y comprenderlos.
- Confirmar lo siguiente:
    - Todas las actualizaciones de seguridad y las características del software del Portal de SecureTrust se incluirán en las actualizaciones de versiones más importantes.
    - El Servicio consiste en una consultoría remota.
    - SecureTrust puede solicitar pruebas de los sistemas y los procesos del Cliente, según sea necesario, para demostrar el cumplimiento con cualquier requisito específico. El Cliente acepta presentar todas las pruebas de forma oportuna.
    - SecureTrust no es responsable de definir los sistemas dentro del alcance ni de establecer si la información proporcionada por el Cliente es precisa.
    - SecureTrust se reserva el derecho de rechazar o aceptar los comentarios del Cliente en función de los hechos y las circunstancias del Servicio.
    - SecureTrust brindará el Servicio en el idioma inglés.
    - SecureTrust no ofrecerá orientación ni asesoramiento legal.
    - La calidad y la precisión del Servicio dependerán de que el Cliente proporcione a SecureTrust información precisa y acceso a sus sistemas y recursos.